#8
E.O.T (1) 4-22-04 mlg

OFFICIAL

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Tugenberg et al.
For:	Method for Purchasing Items Over a Non-Secure Communication Channel
Serial No.:	09/671,941
Filed:	September 27, 2000
Examiner:	Backer, F.
Art Unit:	3621

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Attention: Board of Patent Appeals and Interferences

APPELLANTS' BRIEF

04/22/2004 LWALDEN 00000003 502117 09671941
Sale Ref: 00000003 DAH: 502117 09671941
01 FC:1251 2004.00 DA
02 FC:1402 330.00 DA

This brief is in furtherance of the Notice of Appeal, transmitted on January 12, 2004.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief is being transmitted by facsimile, and therefore the requirement that it be transmitted in triplicate is believed to be waived.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 1.192(c)):

I REAL PARTY IN INTEREST

II RELATED APPEALS AND INTERFERENCES

I. REAL PARTY IN INTEREST

The real party in interest in this appeal is Motorola, Inc., a Delaware corporation.

II. RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in this appeal, there are no such appeals or interferences.

III. STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 19

B. STATUS OF ALL THE CLAIMS

1. Claims canceled: none
2. Claims withdrawn from consideration but not canceled: none
3. Claims pending: 1-19
4. Claims allowed: none
5. Claims objected to: none
6. Clams rejected: 1-19

C. CLAIMS ON APPEAL

The claims on appeal are: 1-19

IV. STATUS OF ANY AMENDMENTS AFTER FINAL

One response, dated February 26, 2004, was filed after the filing of a Notice of Appeal. No amendments were included in the response. As a result, no amendments have been made after final.

V. SUMMARY OF INVENTION

The invention pertains to a secure processing system (14) for storing sensitive data in encrypted form. When the sensitive data is needed e.g. for use in connection with a secure transaction, the sensitive data is decrypted using a laser-scribed encryption key (21) for recovering the sensitive data, such as credit card information and a secret key (page 4, lines 3-7). The decrypted sensitive information is then encrypted using a communication encryption key, which is related to the secret key, and the information is conveyed to the destination in encrypted form (page 8, lines 2-8; 310 FIG. 3; page 14, lines 14-16; and page 16, lines 17-19).

In at least one embodiment, the sensitive data is stored in the non-secure memory in encrypted form (page 7, lines 34 to page 8, line 2). When the data is decrypted, the data is stored in a secure zeroizable memory (28), which can be cleared when any attempt at unauthorized access is attempted (page 5, lines 21-28).

In at least a further embodiment, the laser-scribed key is formed during the manufacturing process (page 3, lines 30-36) in which a randomly generated or otherwise substantially unique code sequence is generated and fixed with some degree of permanence into the circuitry (page 6, lines 8-20). Blocking gates can be used to prevent unauthorized access to the laser-scribed key (page 5, lines 28-33).

VI. ISSUES

1. Whether claims 1-19 have been improperly rejected under 35 U.S.C. 102(c) as being anticipated by Matsushima et al. (US Published Patent Appln. No. 2002/0161722).

A. Whether the record supports a prima facie showing that the cited reference, Matsushima et al., '722, qualifies as prior art.

VII. GROUPING OF CLAIMS

Group 1: Claims 1-19

VIIIA. ARGUMENTS -- REJECTIONS UNDER 35 U.S.C. § 102

The Examiner has rejected claims 1-19 as being anticipated by Matsushima et al., US Patent Application Publication No. 2002/0161722. However the Examiner has failed to establish that the cited reference qualifies as prior art, and consequently that the reference was appropriately cited against the present application. Consequently, the Examiner has failed to present a prima facie case of anticipation, which would necessitate a response by the applicant. In other words, the Examiner's rejection continues to be improperly supported and/or defective, and has never been properly established, such that a response by the applicant would be required.

More specifically, based upon the facts in the record, Matsushima et al., '722, can not be established as a prior reference given the filing date of the corresponding PCT application is January 12, 2001, which is after the filing date September 27, 2000, of the present application. While the applicants acknowledge that the reference identifies a related application, which was filed January 14, 2000, the present application is identified as a continuation-in-part application of the related application with no basis upon facts properly established in the record as to what portions of the presently cited reference may have been originally present or may have been later added.

By definition, a continuation-in-part application implies that additional subject matter has

been added to the application from which the continuation-in-part application claims priority (see MPEP §201.08). Still further, unless the filing date of the earlier nonprovisional application is actually needed, for example, in the case of an interference or to overcome a reference, the MPEP indicates that there is no need to make a determination as to whether the earlier nonprovisional application discloses the invention of the second application. In fact, the Examiners are encouraged to merely insure that the minimal formalities of 35 U.S.C. §120 are met. Still further, the status of the present application is further in doubt given the fact that there is no indication that the cited reference has undergone any form of substantive examination, and therefore there may not have been any opportunity to evaluate the proper priority of the published application, even under the above outlined very limited set of circumstances, in which such an analysis might be required.

In responding to the Applicants' earlier criticism relative to the presently cited reference, the Examiner indicates that he has only **minimally** reviewed the earlier application. Ironically, to the extent that the Examiner attempts to show that the earlier application is directed to a similar scope, the Examiner identifies elements in the earlier application, which have completely different reference numbers that fail to match any of the element/reference numbers in the later application. This would alternatively suggest that the cited reference and the parent application from which it claims at least partial priority, are more different than similar, making it seemingly less likely that the later application is entitled to the earlier filing date. Based upon the Examiner's own admissions relative to the description of the applications provided, the Examiner's showing serves to alternatively suggest that the applications contain substantial differences, and most notably in the specific areas of concern. More importantly the Examiner has failed to establish the presence of the relied upon subject matter as being present in the earlier application by establishing the facts, upon which such a showing would be necessary, as part of the record.

Furthermore, in attempting to justify the appropriateness of the use of the earlier priority date in association with the cited reference, the Examiner fails to provide the complete analysis, which is required to establish the suitability of an association of the earlier priority date with a later filed application. More specifically, in order for a continuation-in-part application to be

entitled to the filing date associated with the parent application, not only must the Examiner show that the teachings being relied upon in support of the rejection are present in the earlier application, but the Examiner must also show that the later filed claims are supported by the earlier specification (please see MPEP §2136.03 IV). No such showing by the Examiner has been made or attempted. As a result, the Examiner has failed to support a showing that the cited reference is entitled to the priority date of the parent application, and consequently has failed to articulate a rejection, which meets the requirements of a prima facie showing of anticipation.

The Examiner bears the burden of presenting at least a prima facie case of anticipation, and it is only when that burden is met, that there is an obligation for the applicant to respond. In re Sun, 31 USPQ2d 1451, 1456 (Fed Cir. 1993). In the present instance no prima facie case of anticipation has been established, and consequently the applicant does not have an obligation, up to this point, to even respond.

To the extent that the Examiner has attempted to allege that the cited reference is entitled to claim priority to the filing date of the parent application, as noted above, the Examiner has relied solely upon alleged facts, which have not been made part of the record. More specifically, the Examiner has relied upon alleged teachings of the parent application, without providing a copy of the parent application to the applicant or including the same as part of the record. To the extent that the Examiner attempts to rely upon facts, which are not part of and/or are not supported in the record, the rejection can only be said to be supported by some form of Official Notice. However Official Notice can only be used to assert well known facts, which are capable of such instant and unquestionable demonstrations as to defy dispute. Such is not the case in the present instance. Furthermore, when the appropriateness of the alleged facts are called into question, as they were in the applicants' response to the initial and re-affirmed rejection, the Examiner is then obligated to provide support for the alleged fact. Here the Examiner has failed to comply with this obligation by failing to produce a copy of the reference from which the Examiner claims support.

In absence of a properly supported rejection, the rejection should be withdrawn, and the application allowed to proceed to issuance. Still further, if withdrawal of the rejection is deemed to be appropriate, and/or the Examiner is required to provide additional support for the present

rejection, in order for the applicants to be given a full and fair opportunity to evaluate the merits of the rejection, and correspondingly an opportunity to respond, should continued examination be deemed to be appropriate, the finality of the rejection should minimally be withdrawn. The applicants would respectfully request the reconsideration and reexamination of the present application in view of the present remarks.

Respectfully submitted,

BY: Lawrence J. Chapa

Lawrence J. Chapa
Reg. No. 39,135
Phone No.: (847) 523-0340

Motorola, Inc.
Personal Communication Sector
Intellectual Property Department
600 North US Highway 45, AS411
Libertyville, IL 60048

IX APPENDIX OF CLAIMS

The following is the text of the claims involved in this appeal:

1. A method for purchasing items over a network using a secure communication device, the secure communication device including a host processor, a secure memory that includes a laser-scribed encryption key, and a non-secure memory for storing encrypted data, wherein sensitive data is encrypted within the secure memory using the laser-scribed encryption key and stored as encrypted data in the non-secure memory, the method comprising the steps of:

retrieving an encrypted credit card number and an encrypted secret key from the non-secure memory;

decrypting the encrypted credit card and secret key with the laser-scribed encryption key;

encrypting the credit card number with a communication encryption key, the communication encryption key being related to the secret key; and

transferring the credit card number, as encrypted with the communication encryption key, over the network to a destination.

2. The method as claimed in claim 1 wherein the encrypted data is decrypted within the secure memory using the laser-scribed encryption key and stored within the secure memory for use by the host processor.

3. The method as claimed in claim 1 further comprising the steps of:

receiving a personal identification number (PIN) from a user;

decrypting an encrypted PIN with the laser-scribed encryption key;

wherein the step of transferring the encrypted credit card number step is performed when the decrypted PIN and the PIN received from the user compare.

4. The method as claimed in claim 1 further comprising the steps of:

receiving biometric information from a user;

decrypting stored biometric information for the user with the laser-scribed encryption key;

wherein the step of transferring the encrypted credit card number step is performed when the decrypted biometric information compares with the biometric information received from the user.

5. The method as claimed in claim 1 wherein the communication encryption key is a common session key and wherein the method further comprises the step of generating the session key using the secret key and information provided by the destination.

6. The method as claimed in claim 1 wherein the host processor and secure memory are fabricated on an integrated circuit chip, and the encrypted data is stored in a non-volatile memory.

7. The method as claimed in claim 1 wherein the laser-scribed encryption key is generated by laser-scribing a semiconductor die during fabrication of the secure memory to create

a plurality of fixed "ones" and "zeroes" which make up the laser-scribed encryption key.

8. The method as claimed in claim 1 wherein the laser-scribed encryption key is generated burning one-time programmable fuses on a semiconductor die during fabrication of the secure memory to create a plurality of fixed "ones" and "zeroes" which make up the laser-scribed encryption key.

9. The method as claimed in claim 1 wherein the secure memory includes blocking gates coupled between the laser-scribed encryption key and encryption logic circuitry, the blocking gates being comprised of logic gates and have a blocking control signal input preventing access to the laser-scribed encryption key by the encryption logic circuitry.

10. The method as claimed in claim 1 wherein the laser-scribed encryption key is unique for each secure memory of a plurality of secure memories of different processing systems.

11. The method as claimed in claim 1 wherein the laser-scribed encryption key is randomly generated for each secure memory of a plurality of secure memories of different processing systems.

12. A method for transferring sensitive data over a non-secure communication channel using a secure communication device, the secure communication device including a host processor, a secure memory that including a laser-scribed encryption key, and a non-secure

memory for storing the sensitive data in encrypted form, wherein sensitive data is encrypted within the secure memory using the laser-scribed encryption key and stored as encrypted data in the non-secure memory, the method comprising the steps of:

retrieving the encrypted sensitive data and an encrypted secret key from the non-secure memory;

decrypting, in the secure memory, the encrypted sensitive data and the secret key with the laser-scribed encryption key;

encrypting the decrypted sensitive data with a session encryption key related to the secret key; and

transferring the sensitive data encrypted with the session encryption key over the non-secure communication channel to a destination.

13. The method as claimed in claim 12 further comprising the steps of:

receiving biometric information from a user;

decrypting stored biometric information for the user with the laser-scribed encryption key;

wherein the step of transferring the encrypted sensitive data step is performed when the decrypted biometric information compares with the biometric information received from the user.

14. The method as claimed in claim 12 wherein the host processor and secure memory are fabricated on an integrated circuit chip, and the encrypted data is stored in a non-volatile

memory.

15. The method as claimed in claim 12 wherein the laser-scribed encryption key is generated by laser-scribing a semiconductor die during fabrication of the secure memory to create a plurality of fixed "ones" and "zeroes" which make up the laser-scribed encryption key.

16. The method as claimed in claim 12 wherein the laser-scribed encryption key is generated by burning one-time programmable fuses on a semiconductor die during fabrication of the secure memory to create a plurality of fixed "ones" and "zeroes" which make up the laser-scribed encryption key.

17. The method as claimed in claim 12 wherein the secure memory includes blocking gates coupled between the laser-scribed encryption key and encryption logic circuitry, the blocking gates being comprised of logic gates and have a blocking control signal input preventing access to the laser-scribed encryption key by the encryption logic circuitry.

18. The method as claimed in claim 12 wherein the laser-scribed encryption key is randomly generated for each secure memory of a plurality of secure memories of different processing systems.

19. The method as claimed in claim 12 wherein the laser-scribed encryption key is unique for each secure memory of a plurality of secure memories of different processing systems.